

08. 7. 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   7 月   8 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 2 7 1 9 2 9  
Application Number:  
[ST. 10/C] :            [ J P 2 0 0 3 - 2 7 1 9 2 9 ]

出   願   人            松 下 電 器 産 業 株 式 会 社  
Applicant(s):

REC'D 26 AUG 2004

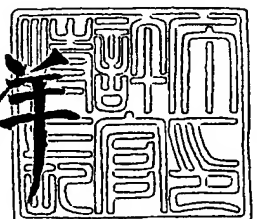
WIPO            PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年   8 月 1 2 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川 洋



【書類名】 特許願  
【整理番号】 2022550237  
【提出日】 平成15年 7月 8日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G09C 1/00  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 中野 稔久  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 館林 誠  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 山本 直紀  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 石原 秀志  
【特許出願人】  
    【識別番号】 000005821  
    【氏名又は名称】 松下電器産業株式会社  
【代理人】  
    【識別番号】 100090446  
    【弁理士】  
    【氏名又は名称】 中島 司朗  
【手数料の表示】  
    【予納台帳番号】 014823  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9003742

**【書類名】 特許請求の範囲****【請求項 1】**

認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、

前記再生装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、

前記読出装置は、前記記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする認証システム。

**【請求項 2】**

前記認証システムであって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、保持する証明書の ID 番号が含まれる 2 つ以上の ID 番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする請求項 1 記載の認証システム。

**【請求項 3】**

前記認証システムであって、

前記読出装置が前記再生装置を認証する認証用データに登録された ID 番号には、2 つ以上の ID 番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする請求項 2 記載の認証システム。

**【請求項 4】**

前記認証システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項 1 記載の認証システム。

**【請求項 5】**

認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、

前記再生装置は、前記読出装置が読み出した第 1 の認証用データを受信する受信部と、前記第 1 の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第 2 の認証用データを受信する受信部と、前記第 2 の認証用データの正当性を検証する検証部と、前記検証後に前記第 2 の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、

前記読出装置は、前記記録媒体から読み出した第 1 の認証用データ、並びに第 2 の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする認証システム。

**【請求項 6】**

前記認証システムであって、

前記読出装置が前記再生装置を認証する前記第 1 の認証用データには、無効化すべき再生装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、保持する証明書の ID 番号が含まれる 2 つ以上の ID 番号を前記認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする請求項5記載の認証システム。

【請求項7】

前記認証システムであって、

前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする請求項6記載の認証システム。

【請求項8】

前記認証システムであって、

前記読出装置が前記再生装置を認証する前記第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、

前記再生装置は、保持する証明書のID番号と一致するID番号を前記第1の認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、

前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする請求項5記載の認証システム。

【請求項9】

前記認証システムであって、

前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする請求項8記載の認証システム。

【請求項10】

前記認証システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項5記載の認証システム。

【請求項11】

コンテンツを再生する再生装置であって、

前記再生装置は、読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする再生装置。

【請求項12】

前記再生装置であって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、

前記再生装置は、保持する証明書のID番号が含まれる2つ以上のID番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする請求項11記載の再生装置。

【請求項13】

コンテンツを再生する再生装置であって、

前記再生装置は、前記読出装置が読み出した第1の認証用データを受信する受信部と、前記第1の認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第2の認証用データを受信する受信部と、前記第2の認証用データの正当性を

検証する検証部と、前記検証後に前記第 2 の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする再生装置。

【請求項 14】

前記再生装置であって、

前記読出装置が前記再生装置を認証する前記第 1 の認証用データには、無効化すべき再生装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、保持する証明書の ID 番号が含まれる 2 つ以上の ID 番号を前記認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第 2 の認証用データには、無効化すべき読出装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、前記読出装置が保持する証明書の ID 番号が前記第 2 の認証用データに登録されているか否かを判定することを特徴とする請求項 13 記載の再生装置。

【請求項 15】

前記再生装置であって、

前記読出装置が前記再生装置を認証する前記第 1 の認証用データには、有効な再生装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、保持する証明書の ID 番号と一致する ID 番号を前記第 1 の認証用データから抽出して前記読出装置に送信して、

前記再生装置が前記読出装置を認証する前記第 2 の認証用データには、無効化すべき読出装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置は、前記読出装置が保持する証明書の ID 番号が前記第 2 の認証用データに登録されているか否かを判定することを特徴とする請求項 13 記載の再生装置。

【請求項 16】

認証用データ、並びにコンテンツを読み出す読出装置であって、

前記読出装置は、記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする読出装置。

【請求項 17】

前記読出装置であって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定する ID 番号が登録され、

前記読出装置が前記再生装置を認証する認証用データに登録された ID 番号には、2 つ以上の ID 番号の組み合わせに対して署名、あるいは認証子が生成され、

前記検証部が検証する前記部分認証用データは、前記 2 つ以上の ID 番号に対する署名、あるいは認証子であることを特徴とする請求項 16 記載の読出装置。

【請求項 18】

認証用データ、並びにコンテンツを読み出す読出装置であって、

前記読出装置は、前記記録媒体から読み出した第 1 の認証用データ、並びに第 2 の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする読出装置。

【請求項 19】

前記読出装置であって、

前記読出装置が前記再生装置を認証する前記第 1 の認証用データには、無効化すべき再生装置が保持する証明書を特定する ID 番号が登録され、

前記再生装置が前記読出装置を認証する前記第 2 の認証用データには、無効化すべき読

出装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する第 1 の認証用データに登録された I D 番号には、2 つ以上の I D 番号の組み合わせに対して署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第 2 の認証用データに対しては、登録された I D 番号全体に対する署名、あるいは認証子が生成され、

前記検証部が検証する前記部分認証用データは、前記 2 つ以上の I D 番号に対する署名、あるいは認証子であることを特徴とする請求項 18 記載の読出装置。

【請求項 20】

前記読出装置であって、

前記読出装置が前記再生装置を認証する前記第 1 の認証用データには、有効な再生装置が保持する証明書を特定する I D 番号が登録され、

前記再生装置が前記読出装置を認証する前記第 2 の認証用データには、無効化すべき読出装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する第 1 の認証用データに登録された I D 番号には、それぞれの I D 番号に対して個別の署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第 2 の認証用データに対しては、登録された I D 番号全体に対する署名、あるいは認証子が生成され、

前記検証部が検証する前記部分認証用データは、前記 I D 番号に対する個別の署名、あるいは認証子であることを特徴とする請求項 18 記載の読出装置。

【請求項 21】

認証用データを記録する記録媒体であって、

前記記録媒体が記録する読出装置が再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する認証用データに登録された I D 番号には、2 つ以上の I D 番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする記録媒体。

【請求項 22】

認証用データを記録する記録媒体であって、

前記記録媒体が記録する読出装置が再生装置を認証する第 1 の認証用データには、無効化すべき再生装置が保持する証明書を特定する I D 番号が登録され、

前記記録媒体が記録する前記再生装置が前記読出装置を認証する第 2 の認証用データには、無効化すべき読出装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する第 1 の認証用データに登録された I D 番号には、2 つ以上の I D 番号の組み合わせに対して署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第 2 の認証用データに対しては、登録された I D 番号全体に対する署名、あるいは認証子が生成されることを特徴とする記録媒体。

【請求項 23】

認証用データを記録する記録媒体であって、

前記記録媒体が記録する読出装置が再生装置を認証する第 1 の認証用データには、有効な再生装置が保持する証明書を特定する I D 番号が登録され、

前記記録媒体が記録する前記再生装置が前記読出装置を認証する第 2 の認証用データには、無効化すべき読出装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する第 1 の認証用データに登録された I D 番号には、それぞれの I D 番号に対して個別の署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第 2 の認証用データに対しては、登録された I D 番号全体に対する署名、あるいは認証子が生成されることを特徴とする記録媒体。

【請求項 24】

読出装置、あるいは再生装置を認証するための認証用データであって、

前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定する I D 番号が登録され、

前記読出装置が前記再生装置を認証する認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項 25】

読出装置、あるいは再生装置を認証するための認証用データであって、

前記読出装置が前記再生装置を認証する第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、

前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、

前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項 26】

読出装置、あるいは再生装置を認証するための認証用データであって、

前記読出装置が前記再生装置を認証する第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、

前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、

前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、

前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする認証用データ。

【請求項 27】

認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、

前記端末装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、

前記読出装置は、前記記録媒体から読み出した認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする認証システム。

【請求項 28】

前記認証システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項 27 記載の認証システム。

【請求項 29】

認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、

前記端末装置は、前記読出装置が読み出した第1の認証用データを受信する受信部と、前記第1の認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第2の認証用データを受信する受信部と、前記第2の認証用データの正当性を検証する検証部と、前記検証後に前記第2の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、

前記読出装置は、前記記録媒体から読み出した第1の認証用データ、並びに第2の認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする認証システム。

【請求項 3 0】

前記認証システムであって、

記録媒体の代わりに通信媒体を利用することを特徴とする請求項 2 9 記載の認証システム。



## 【書類名】明細書

【発明の名称】認証システム、読出装置、再生装置、端末装置、記録媒体、及び認証用データ

## 【技術分野】

## 【0001】

本発明は、公開鍵暗号を利用した認証システムに関するものであり、特に無効化された公開鍵証明書を特定する公開鍵証明書無効化リストを含む認証システムに関する。

## 【背景技術】

## 【0002】

近年、インターネットの急速な広がりにより、インターネットをその通信の基盤とするシステムも増加している。例えば、インターネットを介して物品の売買を行う電子商取引もその1つである。このような、インターネットを通信の基盤とするシステムにおいては、通信相手がシステムの正当な参加者であることを確認することが必須となる。これを認証という。通信相手としては人間が機器を操作している場合や、機器が予め決められた手順で処理を行う場合があるが、以下ではこの両者を含めて機器という。そして通信相手を認証することを機器認証という。なお、機器が正当性、すなわち自分がシステムの正当な参加者であることを示すことを「証明する」といい、相手の正当性を確認することを「検証する」という。認証とは証明と検証の両方を含む言葉とする。

## 【0003】

また、暗号技術には共通鍵暗号と公開鍵暗号がある。共通鍵暗号は暗号化のための鍵と復号のための鍵が同じ物である。一方、公開鍵暗号は暗号化のための鍵と復号のための鍵が異なるものである。認証を行うには公開鍵暗号を用いる方が望ましい。なぜならば、共通鍵暗号を用いた認証においては、検証者は証明者と同じ秘密を持つので、これ以降、検証者が証明者になりすます危険性がある。いわゆるパスワード方式はこれに該当する。公開鍵暗号を用いた認証においては、証明者は公開鍵暗号の秘密鍵を用いて証明し、検証者はその秘密鍵に対する公開鍵を用いて検証するのであり、公開鍵から秘密鍵は作成できないようになっているので、認証が終わった後で、検証者が証明者になりすますことができないからである。

## 【0004】

なお、公開鍵暗号技術において、秘密鍵を用いて処理を行うことを署名といい、対応する公開鍵を用いてその署名の正当性を確認することを検証するという。

## 【0005】

公開鍵暗号を用いた相手認証処理の例として、第1の機器が第2の機器にチャレンジデータとして乱数データを送信し、続いて、第2の機器がその乱数データに対して自分の秘密鍵で署名を行って第1の機器にレスポンスデータを返信し、最後に、返信されてきた署名文に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが当該システム内で有効なものであることが前提となる。

## 【0006】

このために、当該システムにおいて認証局 (Certification Authority: 以下、CA) と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す (公開鍵に対する「お墨付き」となる) 「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、そのデータに対する認証局の電子署名の正しさを確認し、さらに相手機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、システムから排除され、正当ではないとされる機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト (Certificate Revocation List: 以下、CRL) として発行される。

## 【0007】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器の公開鍵証明書を手し、入手した公開鍵証明書がCRLに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な相手機器との取引を回避することができる。なお、CRLの形式、実現例等は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。そのCRLの実現例の一つとしては、特許文献1が開示されており、CRL形式の一例としては、非特許文献1にISO/IEC/ITUが定めたX.509標準で定義されるCRL形式（データ構造）が開示されている。

【特許文献1】特開2003-115838号公報

【特許文献2】特開2002-281013号公報

【非特許文献1】山田慎一郎訳、「デジタル署名と暗号技術」、ピアソン・エデュケーション

【非特許文献2】池野信一、小山謙二、「現代暗号理論」、電子通信学会

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0008】

しかしながら、前記従来の構成で相手の公開鍵証明書の有効性を判断する場合は、相手の公開鍵証明書がCRLに記載されているか否かをチェックして判断する必要がある。このとき、CRLに登録する公開鍵証明書（無効化すべき公開鍵証明書）の数が増加すると、それに伴いCRLのサイズが大きくなり、そのチェックに必要な処理時間も大きくなる。ここで、パソコンのような、ディスクからデータを読み出す読出装置（ドライブ）と読出装置を制御する装置（ホスト）の構成を考えた場合、ホストに比べて処理能力の低いドライブにおいても上記CRLのチェックを行う必要があり、CRLのサイズが大きくなるに従い、ドライブにかかる処理負荷が増加するという課題を有していた。

## 【0009】

本発明は、前記従来の課題を解決するもので、パソコンのドライブとホストのように処理能力に大きな差がある場合に、処理能力の低いドライブにおけるCRLチェックの負荷を軽減させる認証システムを提供することを目的とする。

## 【課題を解決するための手段】

## 【0010】

本発明は、認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、前記再生装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、前記読出装置は、前記記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

## 【0011】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号が含まれる2つ以上のID番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする。

## 【0012】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。

## 【0013】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【0014】

また、本発明は、認証用データと暗号化されたコンテンツを記録する記録媒体と、前記認証用データ、並びに前記コンテンツを読み出す読出装置と、前記コンテンツを再生する再生装置からなる認証システムであって、前記再生装置は、前記読出装置が読み出した第1の認証用データを受信する受信部と、前記第1の認証用データから前記再生装置に係る部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第2の認証用データを受信する受信部と、前記第2の認証用データの正当性を検証する検証部と、前記検証後に前記第2の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、前記読出装置は、前記記録媒体から読み出した第1の認証用データ、並びに第2の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【0015】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号が含まれる2つ以上のID番号を前記認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする。

【0016】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0017】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号と一致するID番号を前記第1の認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする。

【0018】

また、本発明は、前記認証システムであって、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0019】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【0020】

また、本発明は、コンテンツを再生する再生装置であって、前記再生装置は、読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記再生装置に関

係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする。

【0021】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号が含まれる2つ以上のID番号を前記認証用データから抽出して前記読出装置に送信することを特徴とする。

【0022】

また、本発明は、コンテンツを再生する再生装置であって、前記再生装置は、前記読出装置が読み出した第1の認証用データを受信する受信部と、前記第1の認証用データから前記再生装置に係る部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第2の認証用データを受信する受信部と、前記第2の認証用データの正当性を検証する検証部と、前記検証後に前記第2の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部と、前記読出装置からコンテンツを受信する受信部を備えることを特徴とする。

【0023】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号が含まれる2つ以上のID番号を前記認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする。

【0024】

また、本発明は、前記再生装置であって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、前記再生装置は、保持する証明書のID番号と一致するID番号を前記第1の認証用データから抽出して前記読出装置に送信して、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記再生装置は、前記読出装置が保持する証明書のID番号が前記第2の認証用データに登録されているか否かを判定することを特徴とする。

【0025】

また、本発明は、認証用データ、並びにコンテンツを読み出す読出装置であって、前記読出装置は、記録媒体から読み出した認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【0026】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記2つ以上のID番号に対する署名、あるいは認証子であることを特徴とする。

【0027】

また、本発明は、認証用データ、並びにコンテンツを読み出す読出装置であって、前記読出装置は、前記記録媒体から読み出した第1の認証用データ、並びに第2の認証用データを前記再生装置に送信する送信部と、前記再生装置から受信した部分認証用データの正

当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記再生装置が保持する証明書の有効性を判定する判定部と、前記判定後に前記再生装置に前記コンテンツを前記再生装置に送信することを特徴とする。

【0028】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記2つ以上のID番号に対する署名、あるいは認証子であることを特徴とする。

【0029】

また、本発明は、前記読出装置であって、前記読出装置が前記再生装置を認証する前記第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、前記再生装置が前記読出装置を認証する前記第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成され、前記検証部が検証する前記部分認証用データは、前記ID番号に対する個別の署名、あるいは認証子であることを特徴とする。

【0030】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。

【0031】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記記録媒体が記録する前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0032】

また、本発明は、認証用データを記録する記録媒体であって、前記記録媒体が記録する読出装置が再生装置を認証する第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、前記記録媒体が記録する前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0033】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって

、前記読出装置が前記再生装置を認証する認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成されることを特徴とする。

【0034】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって、前記読出装置が前記再生装置を認証する第1の認証用データには、無効化すべき再生装置が保持する証明書を特定するID番号が登録され、前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、2つ以上のID番号の組み合わせに対して署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0035】

また、本発明は、読出装置、あるいは再生装置を認証するための認証用データであって、前記読出装置が前記再生装置を認証する第1の認証用データには、有効な再生装置が保持する証明書を特定するID番号が登録され、前記再生装置が前記読出装置を認証する第2の認証用データには、無効化すべき読出装置が保持する証明書を特定するID番号が登録され、前記読出装置が前記再生装置を認証する第1の認証用データに登録されたID番号には、それぞれのID番号に対して個別の署名、あるいは認証子が生成され、前記再生装置が前記読出装置を認証する第2の認証用データに対しては、登録されたID番号全体に対する署名、あるいは認証子が生成されることを特徴とする。

【0036】

また、本発明は、認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、前記端末装置は、前記読出装置が読み出した認証用データを受信する受信部と、前記認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部を備え、前記読出装置は、前記記録媒体から読み出した認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする。

【0037】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用することを特徴とする。

【0038】

また、本発明は、認証用データを記録する記録媒体と、前記認証用データを読み出す読出装置と、前記認証用データを用いて認証を実行する端末装置からなる認証システムであって、前記端末装置は、前記読出装置が読み出した第1の認証用データを受信する受信部と、前記第1の認証用データから前記端末装置に関係する部分認証用データを抽出する抽出部と、前記抽出した部分認証用データを前記読出装置に送信する送信部と、前記読出装置が読み出した第2の認証用データを受信する受信部と、前記第2の認証用データの正当性を検証する検証部と、前記検証後に前記第2の認証用データを用いて前記読出装置が保持する証明書の有効性を判定する判定部を備え、前記読出装置は、前記記録媒体から読み出した第1の認証用データ、並びに第2の認証用データを前記端末装置に送信する送信部と、前記端末装置から受信した部分認証用データの正当性を検証する検証部と、前記検証後に前記部分認証用データを用いて前記端末装置が保持する証明書の有効性を判定する判定部を有することを特徴とする。

【0039】

また、本発明は、前記認証システムであって、記録媒体の代わりに通信媒体を利用する



ことを特徴とする。

【発明の効果】

【0040】

本発明によれば、処理能力の高い再生装置がCRLの検索を行うことで、読出装置がCRLの検索を行わず、署名検証だけを実施する構成にすることが可能であり、効率のよい認証システムを実現することが可能である。また、その場合に、再生装置が検索するCRLのIDの区間に対して署名を施す、あるいは個々のIDに対して署名を施すことにより、再生装置の不正行為も防止することができる。

【0041】

また、本発明によれば、双方向認証を実施する場合、再生装置による読出装置の認証には、従来から用いられるCRLを利用して再生装置がCRLを検索して、逆に、読出装置による再生装置の認証であっても、再生装置がCRLを検索して、読出装置は検索結果の検証を実施するだけで、再生装置の認証を実施することが可能となるため、効率的な双方向の認証システムを実現することも可能である。

【発明を実施するための最良の形態】

【0042】

以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に係る認証システムの全体構成を示すブロック図である。このシステムは、公開鍵の正当性を示す公開鍵証明書と、無効化した公開鍵証明書の一覧を示す公開鍵証明書無効化リスト（以下、CRL）を発行する公開鍵証明書認証局（以下、CA）の端末装置101と、前記発行されたCRLと、暗号化されたコンテンツ（以下、暗号化コンテンツ）を記録する記録媒体102と、前記記録媒体102からCRL、及び暗号化コンテンツを読み出す読出装置103と、前記読出装置103と認証を行い、前記暗号化コンテンツを復号して再生する再生装置104からなる。

【0043】

ただし、CAの端末装置101は、無効化する公開鍵証明書が発生するごとにCRLを更新して記録媒体102に記録する、あるいは前記記録媒体102を製造する製造メーカーに更新したCRLを配布するものとする。また、読出装置103と再生装置104は、汎用の通信路で接続されており、一方が他方を認証する片方向認証、あるいは両者が互いに認証し合う相互認証を実施した後、認証結果がOKであれば、読出装置103は、暗号化コンテンツを再生装置104へ送信し、再生装置104がコンテンツの再生を行う。ここで、汎用の通信路とは、その仕様が公開されているため、通信路上のデータ盗聴、改ざん、差し替えなどの危険に晒される安全でない通信路のことである。

【0044】

（実施の形態1）

図2は、本発明の実施の形態1における、読出装置103が再生装置104を認証する片方向認証の場合の読出装置103、並びに再生装置104の機能を示す機能ブロック図である。

【0045】

読出装置103は、CAの公開鍵を格納するCA公開鍵格納部201と、前記CAの公開鍵を用いてCAが付与した署名の正当性を検証する署名検証部202と、記録媒体102に記録されているCRLと、再生装置104から受信したCRLのバージョン番号が一致するか否かを比較する比較部203と、再生装置104から受信した証明書、並びにCRLを用いて、前記証明書が有効であるか否かを判定する有効性判定部204と、読出装置103と再生装置104を接続する汎用通信路上で情報を安全に送信（暗号化して送信）するために必要なセッション鍵を生成するセッション鍵生成部205と、前記セッション鍵を再生装置104から受信した証明書に含まれる公開鍵で暗号化する暗号化部206と、記録媒体102に記録されている暗号化コンテンツ鍵を前記セッション鍵で暗号化する暗号化部207を備える。

【0046】

再生装置 104 は、自身の証明書を格納する証明書格納部 211 と、読出装置 103 を経由して記録媒体 102 に記録されている再生装置認証用 CRL を受信して、前記証明書をを用いて前記再生装置認証用 CRL を検索して、該当する ID の区間、バージョン番号、それらに対する署名を抽出する検索／抽出部 212 と、前記 CRL から抽出した情報と、前記証明書を読出装置 103 へ送信する証明書／再生装置認証用 CRL 送信部 213 と、再生装置 104 が保持する証明書に含まれる公開鍵に対応する秘密鍵を格納する秘密鍵格納部 214 と、読出装置 103 から受信した暗号化セッション鍵を用いて復号する復号部 215 と、同じく読出装置 103 から受信した 2 重暗号化されたコンテンツ鍵を用いて復号して得たセッション鍵を用いて復号する復号部 216 と、再生装置 104 が保持するデバイス鍵を格納するデバイス鍵格納部 217 と、読出装置 103 を経由して記録媒体 102 に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部 218 と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部 219 と、読出装置 103 を経由して記録媒体 102 に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵を用いて復号してコンテンツを獲得する復号部 220 を備える。

【0047】

また、記録媒体 102 には、暗号化メディア鍵 231、再生装置認証用 CRL 232、暗号化コンテンツ鍵 233、暗号化コンテンツ 234 が記録されている。

【0048】

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献 2 が開示されている。

【0049】

次に、記録媒体 102 に記録される各種データのデータ形式について、図 3 を用いて説明する。

【0050】

記録媒体 102 は、再生装置用 CRL を記録する再生装置用 CRL 記録領域 301 と、暗号化メディア鍵を記録する暗号化メディア鍵記録領域 302 と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域 303 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 304 を備える。

【0051】

再生装置認証用 CRL は、バージョン番号 (VN)、無効化する証明書の ID (RID)、及びそれらの正当性を証明する CA の署名により構成される。図 3 は、3 番の ID を持つ証明書と 10 番の ID を持つ証明書が無効化されている場合の例を示している。このとき、実際の証明書には割り当てない 0 番と 9999 番の ID も合わせて CRL に対して記録される。また、バージョン番号は、CRL が更新された場合に 1 ずつカウントアップされる値である。さらに、CA の署名は、バージョン番号と連続する証明書の ID を連結した値に対して付与される。ただし、記号「||」は、データを連結することを意味する記号として用い、関数  $\text{Sig}(X, Y)$  は、データ Y に対して、鍵データ X を用いて署名生成を行う関数として用いる。また、 $\text{SK\_CA}$  は CA だけが保持する署名生成に利用する秘密鍵のことである。

【0052】

暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵 (DK) ではメディア鍵 ( $K_m$ ) を暗号化して、メディア鍵を与えない装置が持つデバイス鍵 (DK) ではメディア鍵とは全く無関係なダミーデータを暗号化する。図 3 は、DK3 を持つ装置と、DK10 を持つ装置に対してはメディア鍵を与えない場合の例を示している。ただし、関数  $E(X, Y)$  は、データ Y を鍵データ X を用いて暗号化する関数として用いる。

【0053】

暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コ



コンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。

【0054】

次に、図4～図6を用いて、読出装置103と再生装置104の動作について説明する。

【0055】

S401:再生装置104は、読出装置103を経由して記録媒体102から再生装置認証用CRLを受信する。

【0056】

S402:再生装置104は、受信したCRLから、自身が保持する証明書のIDが含まれる区間を検索して、区間、CRLのバージョン番号、及びそれらに対する署名を抽出する。例えば、図3に示す記録媒体102の場合、再生装置104が保持する証明書のIDが5番であれば、CRLのバージョン番号 VN=0001、区間 RID2=0003～RID3=0010、及びそれらに対する署名 Sig (SK\_CA, VN||RID2||RID3) を抽出する。また、再生装置104が保持する証明書のIDが3番であれば、CRLのバージョン番号 VN=0001、区間 RID1=0000～RID2=0003、もしくはRID2=0003～RID3=0005、及びそれらに対する署名 Sig (SK\_CA, VN||RID1||RID2) 、もしくはSig (SK\_CA, VN||RID2||RID3) を抽出する。

【0057】

S403:再生装置104は、S402で抽出した各種データ、及び保持する証明書を読出装置103へ送信する。

【0058】

S404:読出装置103は、再生装置104から受信した証明書、及び署名を、保持するCAの公開鍵を用いて検証する。

【0059】

S405:S404で検証を実行した結果、検証OKであればS501へ、検証NGであれば処理を中止する。

【0060】

S501:読出装置103は、再生装置104から受信したCRLのバージョン番号と、記録媒体102に記録されているバージョン番号が一致するか否かを比較する。

【0061】

S502:S501で比較を実行した結果、一致であればS503へ、不一致であれば処理を中止する。

【0062】

S503:読出装置103は、S404、並びにS501で検証/比較した再生装置104の証明書、並びに再生装置104により抽出されたCRLの一部を用いて、証明書が有効か否かを判定する。例えば、IDが5番の証明書を保持する再生装置104が、区間 RID2=0003～RID3=0010を送信してきた場合は、値5は区間3～10(4, 5, 6, 7, 8, 9)に含まれるためその証明書を有効と判断する。また、IDが3番の証明書を保持する再生装置104が、区間 RID2=0003～RID3=0010を送信してきた場合は、値3は区間3～10には含まれないためその証明書を無効と判断する。

【0063】

S504:S503で判定を実行した結果、有効であればS505へ、無効であれば処理を中止する。

【0064】

S505:読出装置103は、汎用通信路上でデータを安全に送信(暗号化して送信)するためのセッション鍵を生成して、再生装置104から受信した証明書に含まれる公開鍵を用いて暗号化して再生装置104へ送信する。

【0065】

S506:再生装置104は、読出装置103から受信した暗号化セッション鍵を、証明書に含まれる公開鍵に対応する秘密鍵で復号してセッション鍵を得る。

【0066】

S601: 読出装置103は、S505で生成したセッション鍵を用いて、記録媒体102に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置104へ送信する。

【0067】

S602: 再生装置104は、読出装置103から受信した2重暗号化されたコンテンツ鍵を、S506で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【0068】

S603: 再生装置104は、読出装置103を経由して記録媒体102から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、S602で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

【0069】

S604: 再生装置104は、読出装置103を経由して記録媒体102から暗号化コンテンツを受信して、S603で得たコンテンツ鍵で復号してコンテンツを得る。

【0070】

以上に示したように、従来では、読出装置が再生装置を認証する場合、読出装置がCRLを検索しなければならないが、本発明の構成では、読出装置はCRLの検索を行わず、再生装置が検索したCRLの確認(検証)を実行するだけでよく、処理能力の低い読取装置であっても認証処理を効率的に行うことが可能となる。

【0071】

(実施の形態2)

図7は、本発明の実施の形態2における、読出装置700と再生装置720が相互認証を実行する場合の読出装置700、並びに再生装置720の機能を示す機能ブロック図である。

【0072】

読出装置700は、CAの公開鍵を格納するCA公開鍵格納部701と、前記CAの公開鍵を用いてCAが付与した署名の正当性を検証する署名検証部702と、記録媒体740に記録されているCRLと、再生装置720から受信したCRLのバージョン番号が一致するか否かを比較する比較部703と、再生装置720から受信した証明書、並びにCRLを用いて、前記証明書が有効であるか否かを判定する有効性判定部704と、自身の証明書を格納する証明書格納部705と、前記証明書を再生装置720へ送信する証明書送信部706と、読出装置103と再生装置104を接続する汎用通信路上で情報を安全に送信するための認証付き通信路(Secure Authentication Channel:SAC)を確立するのに必要な認証/鍵共有処理を実行する公開鍵暗号処理部707と、記録媒体740に記録されている暗号化コンテンツを前記処理で共有したセッション鍵で暗号化する暗号化部708を備える。

【0073】

再生装置720は、自身の証明書を格納する証明書格納部721と、読出装置700を経由して記録媒体740に記録されている再生装置認証用CRLを受信して、前記証明書を用いて前記再生装置認証用CRLを検索して、該当するIDの区間、バージョン番号、それらに対する署名を抽出する検索/抽出部722と、前記CRLから抽出した情報と、前記証明書を読出装置700へ送信する証明書/再生装置認証用CRL送信部723と、CAの公開鍵を格納するCA公開鍵格納部724と、前記CAの公開鍵を用いてCAが付与した署名の正当性を検証する署名検証部725と、読出装置700から受信した証明書、並びに読出装置700を経由して記録媒体740から受信した読出装置認証用CRLを用いて、前記証明書が有効であるか否かを判定する有効性判定部726と、再生装置720と読出装置700を接続する汎用通信路上で情報を安全に送信するための認証付き通信路(Secure Authentication Channel:SAC)を確立するのに必要な認証/鍵共有処理を実行する公開鍵暗号処理部727と、読出装置700から受信した2重暗号化されたコンテンツ鍵を前記処理で共有したセッション鍵で復号する復号部728と、再生装置720が保持するデバイス鍵を格納するデバイス鍵格納部729と、読出装置700を経由して

記録媒体 740 に記録されている暗号化メディア鍵を受信して、前記デバイス鍵を用いて復号する復号部 730 と、前記復号して得た暗号化コンテンツ鍵を、同じく前記復号して得たメディア鍵で復号する復号部 731 と、読出装置 700 を経由して記録媒体 740 に記録されている暗号化コンテンツを受信して、前記コンテンツ鍵で復号してコンテンツを獲得する復号部 732 を備える。

【0074】

また、記録媒体 740 には、暗号化メディア鍵 741、再生装置認証用 CRL 742、読出装置認証用 CRL 743、暗号化コンテンツ鍵 744、暗号化コンテンツ 745 が記録されている。

【0075】

なお、ある特定の装置にだけメディア鍵を与える方法は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、木構造を利用して鍵を管理する特許文献 2 が開示されている。

【0076】

次に、記録媒体 740 に記録される各種データのデータ形式について、図 8 を用いて説明する。

【0077】

記録媒体 740 は、再生装置認証用 CRL を記録する再生装置認証用 CRL 記録領域 801 と、読出装置認証用 CRL を記録する読出装置認証用 CRL 記録領域 802 と、暗号化メディア鍵を記録する暗号化メディア鍵記録領域 803 と、暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域 804 と、暗号化コンテンツを記録する暗号化コンテンツ記録領域 805 を備える。

【0078】

再生装置認証用 CRL は、バージョン番号 (VN)、無効化する証明書の ID (RID)、及びそれらの正当性を証明する CA の署名により構成される。図 8 は、3 番の ID を持つ証明書と 10 番の ID を持つ証明書が無効化されている場合の例を示している。このとき、実際の証明書には割り当てない 0 番と 9999 番の ID も合わせて CRL に対して記録される。また、バージョン番号は、CRL が更新された場合に 1 ずつカウントアップされる値である。さらに、CA の署名は、バージョン番号と連続する証明書の ID を連結した値に対して付与される。

【0079】

読出装置認証用 CRL は、バージョン番号 (VN')、無効化する証明書の ID (RID')、及びそれら全体の正当性を証明する CA の署名により構成される。図 8 は、1 番の ID を持つ証明書、6 番の ID を持つ証明書、及び 15 番の ID を持つ証明書が無効化されている場合の例を示している。

【0080】

暗号化メディア鍵は、ある特定の装置にだけメディア鍵を与えるためのデータであり、メディア鍵を与える装置が持つデバイス鍵 (DK) ではメディア鍵 (Km) を暗号化して、メディア鍵を与えない装置が持つデバイス鍵 (DK) ではメディア鍵とは全く無関係なダミーデータを暗号化する。図 8 は、DK3 を持つ装置と、DK10 を持つ装置に対してはメディア鍵を与えない場合の例を示している。

【0081】

暗号化コンテンツ鍵は、前記メディア鍵で暗号化されたコンテンツ鍵であり、暗号化コンテンツは前記コンテンツ鍵で暗号化されたコンテンツである。

【0082】

次に、図 9～図 12 を用いて、読出装置 700 と再生装置 720 の動作について説明する。

【0083】

S901: 再生装置 720 は、読出装置 700 を経由して記録媒体 740 から再生装置認証用 CRL を受信する。

## 【0084】

S902:再生装置720は、受信したCRLから、自身が保持する証明書のIDが含まれる区間を検索して、区間、CRLのバージョン番号、及びそれらに対する署名を抽出する。例えば、図8に示す記録媒体740の場合、再生装置720が保持する証明書のIDが5番であれば、CRLのバージョン番号 VN=0001、区間 RID2=0003~RID3=0010、及びそれらに対する署名 Sig (SK\_CA, VN||RID2||RID3)を抽出する。また、再生装置720が保持する証明書のIDが3番であれば、CRLのバージョン番号 VN=0001、区間 RID1=0000~RID2=0003、もしくはRID2=0003~RID3=0005、及びそれらに対する署名 Sig (SK\_CA, VN||RID1||RID2)、もしくはSig (SK\_CA, VN||RID2||RID3)を抽出する。

## 【0085】

S903:再生装置720は、S902で抽出した各種データ、及び保持する証明書を読出装置700へ送信する。

## 【0086】

S904:読出装置700は、再生装置720から受信した証明書、及び署名を、保持するCAの公開鍵を用いて検証する。

## 【0087】

S905:S904で検証を実行した結果、検証OKであればS1001へ、検証NGであれば処理を中止する。

## 【0088】

S1001:読出装置700は、再生装置720から受信したCRLのバージョン番号と、記録媒体740に記録されているバージョン番号が一致するか否かを比較する。

## 【0089】

S1002:S1001で比較を実行した結果、一致であればS1003へ、不一致であれば処理を中止する。

## 【0090】

S1003:読出装置700は、S904、並びにS1001で検証/比較した再生装置720の証明書、並びに再生装置720により抽出されたCRLの一部を用いて、証明書が有効か否かを判定する。例えば、IDが5番の証明書を保持する再生装置720が、区間 RID2=0003~RID3=0010を送信してきた場合は、値5は区間3~10(4, 5, 6, 7, 8, 9)に含まれるためその証明書を有効と判断する。また、IDが3番の証明書を保持する再生装置720が、区間 RID2=0003~RID3=0010を送信してきた場合は、値3は区間3~10には含まれないためその証明書を無効と判断する。

## 【0091】

S1004:S1003で判定を実行した結果、有効であればS1005へ、無効であれば処理を中止する。

## 【0092】

S1005:読出装置700は、保持する自身の証明書を再生装置740へ送信する。

## 【0093】

S1101:再生装置720は、読出装置700から受信した証明書、及び読出装置700を経由して記録媒体740から受信した読出装置認証用CRLに付与されている署名をCAの公開鍵を用いて検証する。

## 【0094】

S1102:S1101で検証を実行した結果、検証OKであればS1103へ、検証NGであれば処理を中止する。

## 【0095】

S1103:再生装置720は、受信した証明書、並びに読出装置認証用CRLを用いて、証明書が有効か否かを判定する。例えば、IDが5番の証明書を保持する読出装置700が、読出装置認証用CRLを送信してきた場合は、値5は受信したCRLに登録されていないためその証明書を有効と判断する。また、IDが6番の証明書を保持する読出装置700が、読出装置認証用CRLを送信してきた場合は、値6は受信したCRLに登録

されているためその証明書を無効と判断する。

【0096】

S1104: S1103で判定を実行した結果、有効であればS1105/S1106へ、無効であれば処理を中止する。

【0097】

S1105/S1106: 読出装置700と再生装置720の間では、両者の公開鍵暗号化処理部が動作してSACを確立し、データの受け渡しはSACを介して安全に行われる。このSACの実現方法については、後に詳細を述べる。SAC処理の結果として、両者はセッション鍵を共有する。

【0098】

S1201: 読出装置700は、S1106で生成したセッション鍵を用いて、記録媒体740に記録されている暗号化コンテンツ鍵をさらに暗号化して再生装置720へ送信する。

【0099】

S1202: 再生装置720は、読出装置700から受信した2重暗号化されたコンテンツ鍵を、S1105で得たセッション鍵で復号して暗号化コンテンツ鍵を得る。

【0100】

S1203: 再生装置720は、読出装置700を経由して記録媒体740から暗号化メディア鍵を受信して、保持するデバイス鍵で復号してメディア鍵を得る。さらに、S1202で得た暗号化コンテンツ鍵を前記メディア鍵で復号してコンテンツ鍵を得る。

【0101】

S1204: 再生装置720は、読出装置700を経由して記録媒体740から暗号化コンテンツを受信して、S1203で得たコンテンツ鍵で復号してコンテンツを得る。

【0102】

以上に示したように、従来では、読出装置と再生装置が相互認証を実行する場合、読出装置もCRLを検索しなければならないが、本発明の構成では、読出装置が再生装置を認証する場合は、読出装置はCRLの検索を行わず、再生装置が検索したCRLの確認(検証)を実行するだけでよく、逆に、再生装置が読出装置を認証する場合もまた、再生装置がCRLの検索を行うため、処理能力の低い読取装置であっても相互認証処理を効率的に行うことが可能となる。

【0103】

次に、読出装置700と再生装置720との間で設定されるSACの実現方法について図13を用いて説明する。ただし、 $\text{Sign}()$ を署名生成関数、 $\text{Veri}()$ を署名検証関数、 $\text{Gen}()$ を鍵生成関数とし、 $Y$ をそのシステム固有のシステムパラメータとする。また、鍵生成関数 $\text{Gen}()$ は、 $\text{Gen}(x, \text{Gen}(y, z)) = \text{Gen}(y, \text{Gen}(x, z))$ の関係を満たすものとする。なお、このような鍵生成関数は、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、非特許文献2に、ディフィーヘルマン(DH)型公開鍵配送法が開示されている。

【0104】

S1301: 読出装置Aは、CAが発行した証明書 $\text{Cert\_A}$ を再生装置Bに送信する。ここでは、証明書の構成要素は、Aの公開鍵 $\text{PK\_A}$ 、AのID( $\text{ID\_A}$ )、それらに対するCAの署名 $\text{Sig\_CA}$ としている。

【0105】

S1302: 再生装置Bは、CAの公開鍵 $\text{P\_CA}$ を用いて $\text{Cert\_A}$ に付与されている署名 $\text{Sig\_CA}$ が正しいか否かを検証する。検証結果が正しくない場合、SACの設定処理を終了する。さらに、再生装置Bは、読出装置AのID( $\text{ID\_A}$ )が、CRLに登録されているか否かを確認する。登録されている場合も、SACの設定処理を終了する。

【0106】

S1303: 再生装置Bは、CAが発行した証明書 $\text{Cert\_B}$ を読出装置Aに送信す

る。ここでは、証明書の構成要素は、Bの公開鍵 $PK\_B$ 、BのID( $ID\_B$ )、それらに対するCAの署名 $Sig\_CA$ としている。

【0107】

S1304: 読出装置Aは、CAの公開鍵 $P\_CA$ を用いて $Cert\_B$ に付与されている署名 $Sig\_CA$ が正しいか否かを検証する。検証結果が正しくない場合、SACの設定処理を終了する。さらに、読出装置Aは、再生装置BのID( $ID\_B$ )が、CRLに登録されているか否かを確認する。登録されている場合も、SACの設定処理を終了する。

【0108】

S1305: 読出装置Aは、乱数 $Cha\_A$ を生成して、再生装置Bに送信する。

【0109】

S1306: 再生装置Bは、受信した $Cha\_A$ に対して、自身の秘密鍵 $SK\_B$ で署名 $Sig\_B$ を生成して、読出装置Aに送信する。

【0110】

S1307: 読出装置Aは、S1303で受信した再生装置Bの公開鍵 $PK\_B$ を用いて、 $Sig\_B$ が正しいか否かを検証する。検証結果が正しくない場合、SACの設定処理を終了する。

【0111】

S1308: 再生装置Bは、乱数 $Cha\_B$ を生成して、読出装置Aに送信する。

【0112】

S1309: 読出装置Aは、受信した $Cha\_B$ に対して、自身の秘密鍵 $SK\_A$ で署名 $Sig\_A$ を生成して、再生装置Bに送信する。

【0113】

S1310: 再生装置Bは、S1301で受信した読出装置Aの公開鍵 $PK\_A$ を用いて、 $Sig\_A$ が正しいか否かを検証する。検証結果が正しくない場合、SACの設定処理を終了する。

【0114】

S1311: 再生装置Bは、乱数 $b$ を生成し、 $Key\_B=Gen(b, Y)$ を計算して読出装置Aに送信する。

【0115】

S1312: 読出装置Aは、乱数 $a$ を生成し、 $Key\_A=Gen(a, Y)$ を計算して再生装置Bに送信する。さらに、読出装置Aは、両者で共有する鍵 $Key\_AB=Gen(b, Key\_A)$ を算出する。

【0116】

S1313: 再生装置Bは、両者で共有する鍵 $Key\_AB=Gen(a, Key\_B)$ を算出する。

【0117】

(その他の変形例)

(1) 本発明の実施の形態1、及び実施の形態2では、再生装置認証用CRLのデータ形式を、無効化する証明書のIDを記載する際、その先頭を最後にダミーのIDを設けてIDの区間に対して署名を生成する形態としたが、本発明はその構成に限定されるものではない。例えば、図14に示すような再生装置認証用CRLの構成であってもよい。図14の再生装置認証用CRLは、ダミーのIDは設けずに、先頭のIDに対しては、そのID単独に署名を施し、以降はIDの区間に対して署名を施す。そして、最後のIDに対しても、そのID単独に署名を施す。このような構成にすることで、読出装置が再生装置の証明書の有効性を確認できるという効果を残しつつ、再生装置認証用CRLのサイズを小さくすることが可能となる。

【0118】

(2) 本発明の実施の形態1、及び実施の形態2では、再生装置認証用CRLを利用して読出装置が再生装置を認証する形態としたが、本発明はその構成に限定されるものではない。例えば、図15に示すような再生装置認証用リストを利用して認証する構成であってもよい。図15の再生装置認証用リストは、無効化すべき証明書のIDではなく、有効

な証明書のIDをリストに登録して、バージョン番号と各有効なIDを連結したデータに対して署名を施したものである。再生装置は、前記再生装置認証用リストを検索して、自身が保持する証明書のIDと一致するIDを抽出して、バージョン番号、抽出したID、それらに対する署名を読出装置へ送信する。読出装置は、受信した署名を検証する。

【0119】

(3) 本発明の実施の形態1、及び実施の形態2では、記録媒体には予め暗号化されたコンテンツが記録されているDVD-Videoのようなプリレコーディッドメディアの形態としたが、本発明はその構成に限定されるものではない。例えば、DVD-RAMのようなレコダブルメディアであってもよい。その場合、実施の形態1、及び実施の形態2と同様に認証を実行した後で、暗号化されたコンテンツを記録する形態となる。

【0120】

(4) 本発明の実施の形態1、及び実施の形態2では、認証に用いるデータ、及びコンテンツが記録媒体に記録される形態としたが、本発明はその構成に限定されるものではない。記録媒体の代わりに通信媒体を利用して、通信媒体を介して、認証に用いるデータ、及びコンテンツを受け渡しする構成であってもよい。また、記録媒体、並びに通信媒体を併用する形態であってもよい。

【0121】

(5) 本発明の実施の形態1、及び実施の形態2では、認証に用いるデータの保護にCAの署名を用いる形態としたが本発明はその構成に限定されるものではない。例えば、読出装置は読出装置専用の秘密鍵を保持し、再生装置は再生装置専用の秘密鍵を用いる構成として、認証に用いるデータには、各秘密鍵を利用して生成された認証子を付与する構成であってもよい。

【産業上の利用可能性】

【0122】

本発明にかかる認証システムは、処理能力の低い読出装置等が含まれる認証システムであっても、効率的な認証を実現できるという効果を有し、公開鍵暗号を利用した認証システムにおいて、特に無効化された公開鍵証明書を特定する公開鍵証明書無効化リストを含む認証システム等において有用である。

【図面の簡単な説明】

【0123】

【図1】 本発明に係る認証システムの全体構成を示すブロック図

【図2】 本発明の実施の形態1における機能ブロック図

【図3】 本発明の実施の形態1における記録媒体に記録されるデータの例を示す図

【図4】 本発明の実施の形態1における動作を示す図

【図5】 本発明の実施の形態1における動作を示す図

【図6】 本発明の実施の形態1における動作を示す図

【図7】 本発明の実施の形態2における機能ブロック図

【図8】 本発明の実施の形態2における記録媒体に記録されるデータの例を示す図

【図9】 本発明の実施の形態2における動作を示す図

【図10】 本発明の実施の形態2における動作を示す図

【図11】 本発明の実施の形態2における動作を示す図

【図12】 本発明の実施の形態2における動作を示す図

【図13】 本発明の実施の形態2における相互認証の例を示す図

【図14】 本発明に係る認証システムにおける記録媒体に記録されるデータの例を示す図

【図15】 本発明に係る認証システムにおける記録媒体に記録されるデータの例を示す図

【符号の説明】

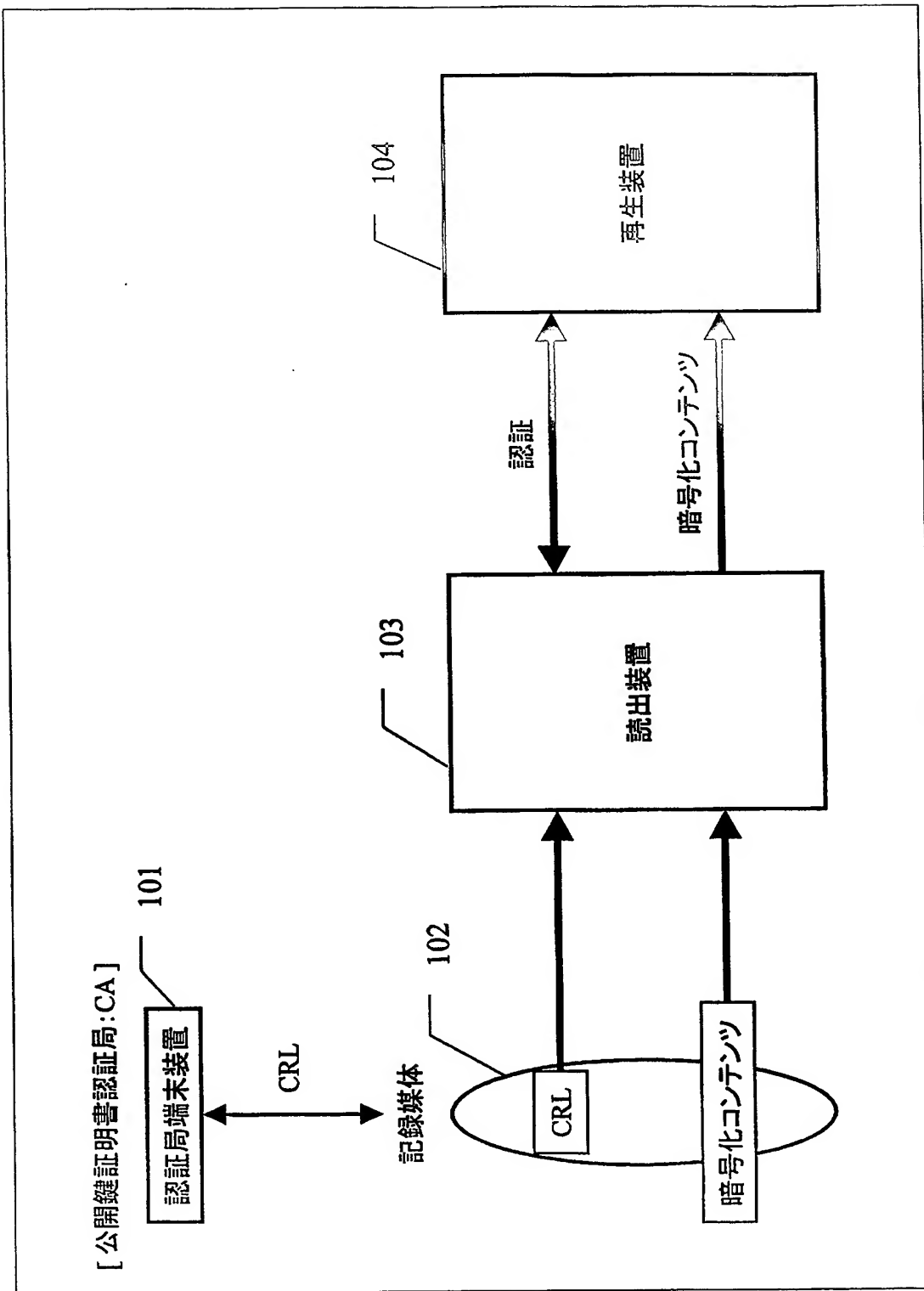
【0124】

101 認証局端末装置

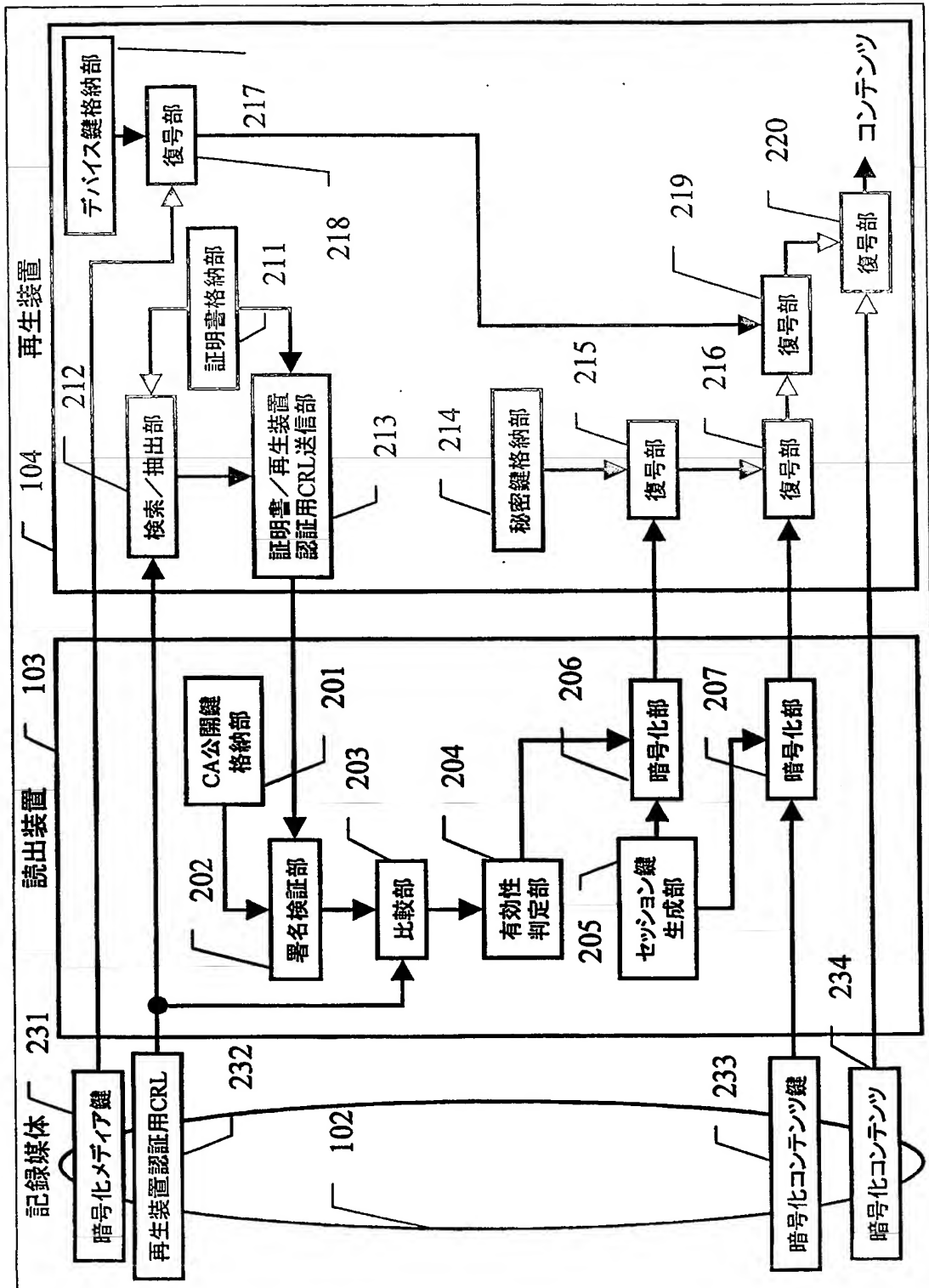
- 1 0 2 記録媒体
- 1 0 3 読出装置
- 1 0 4 再生装置



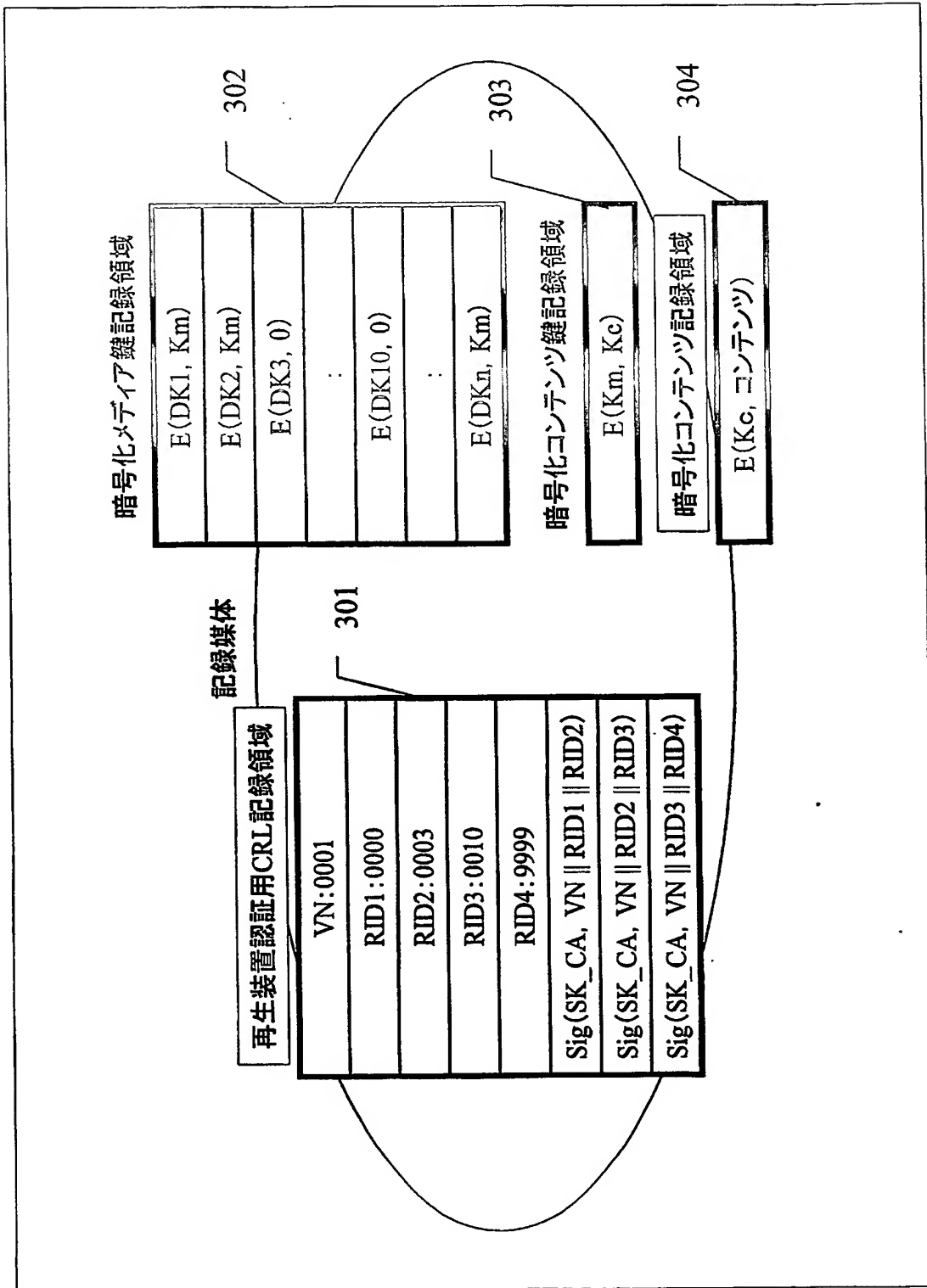
【書類名】 図面  
【図 1】



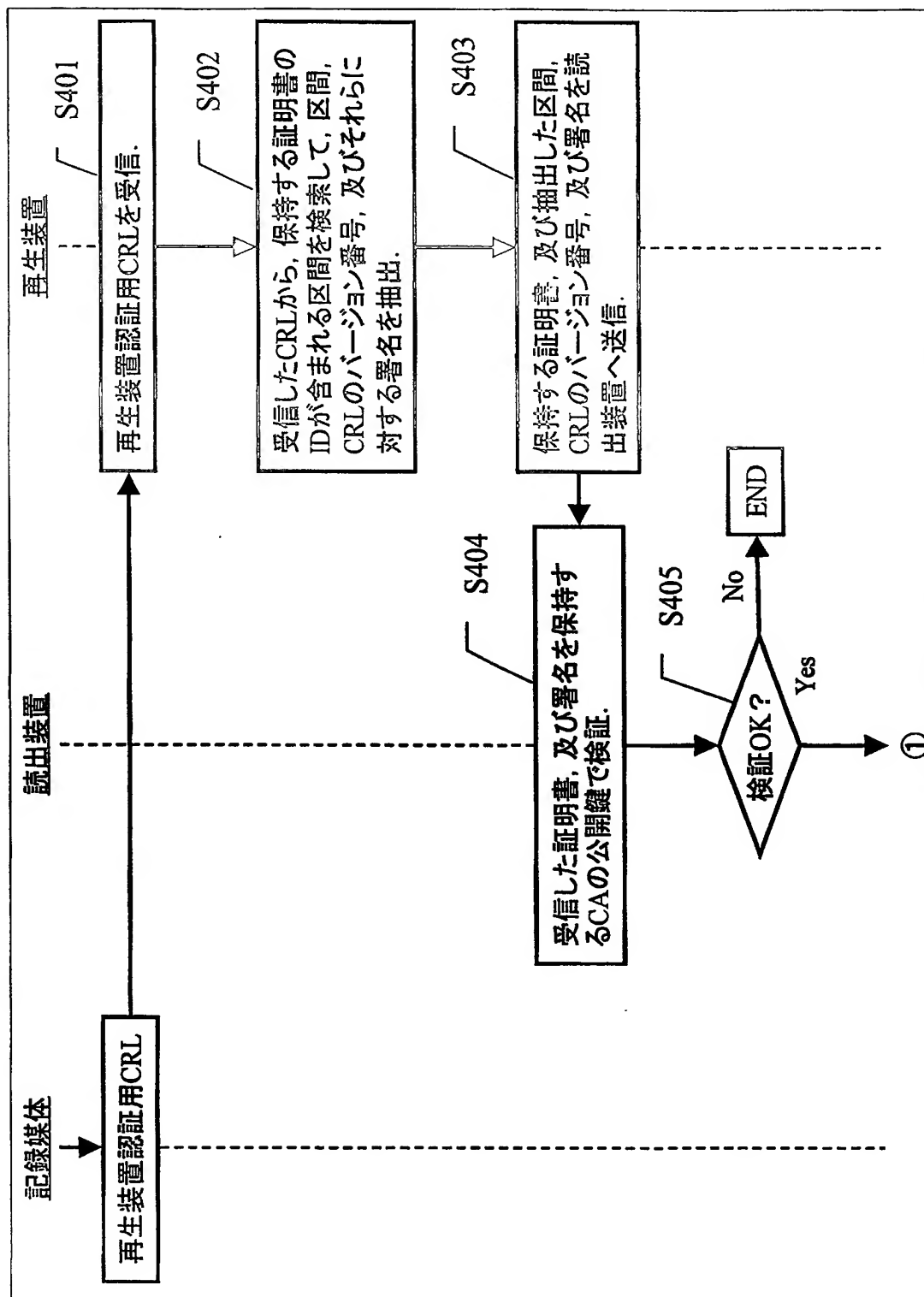
【図 2】



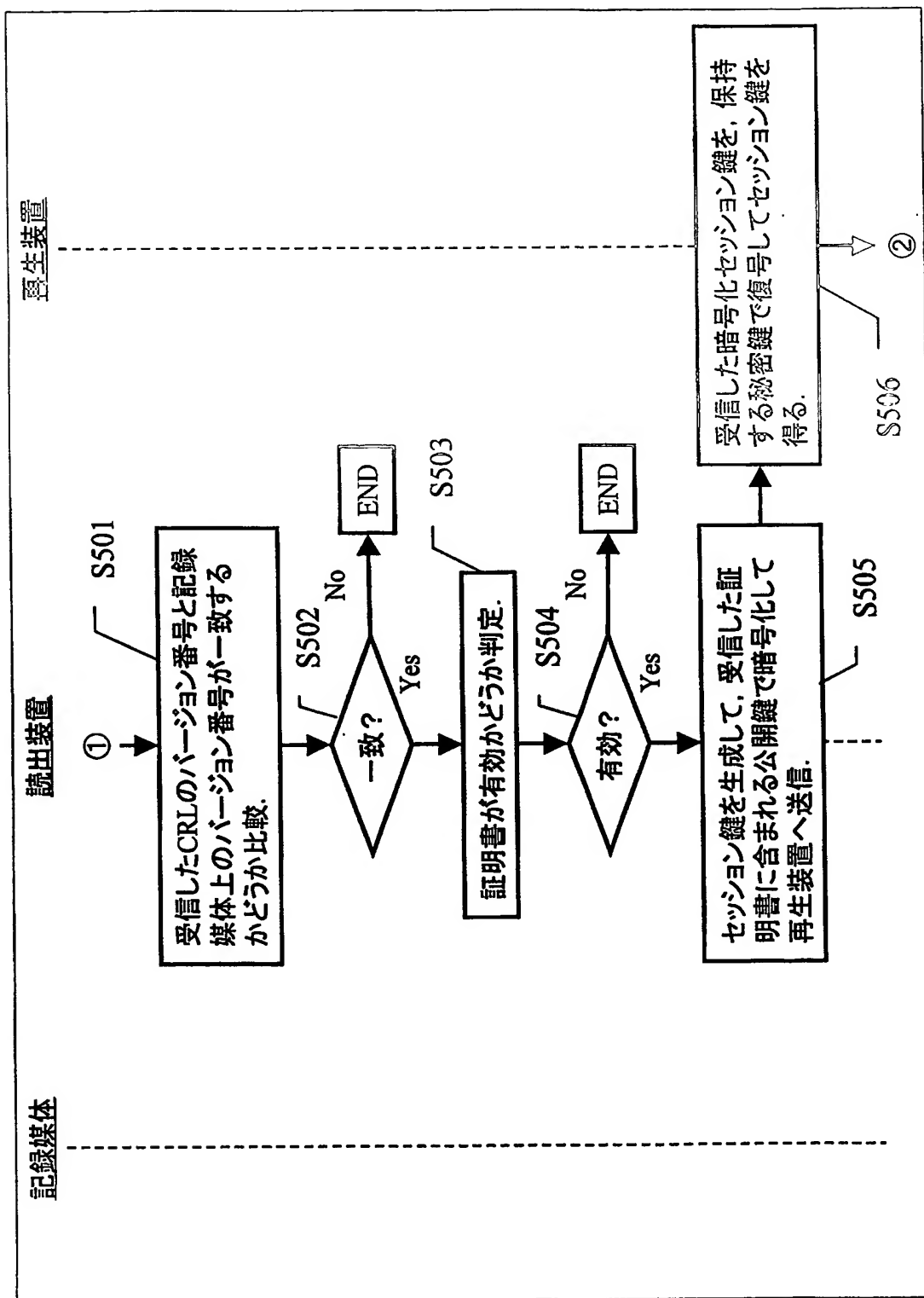
【図 3】



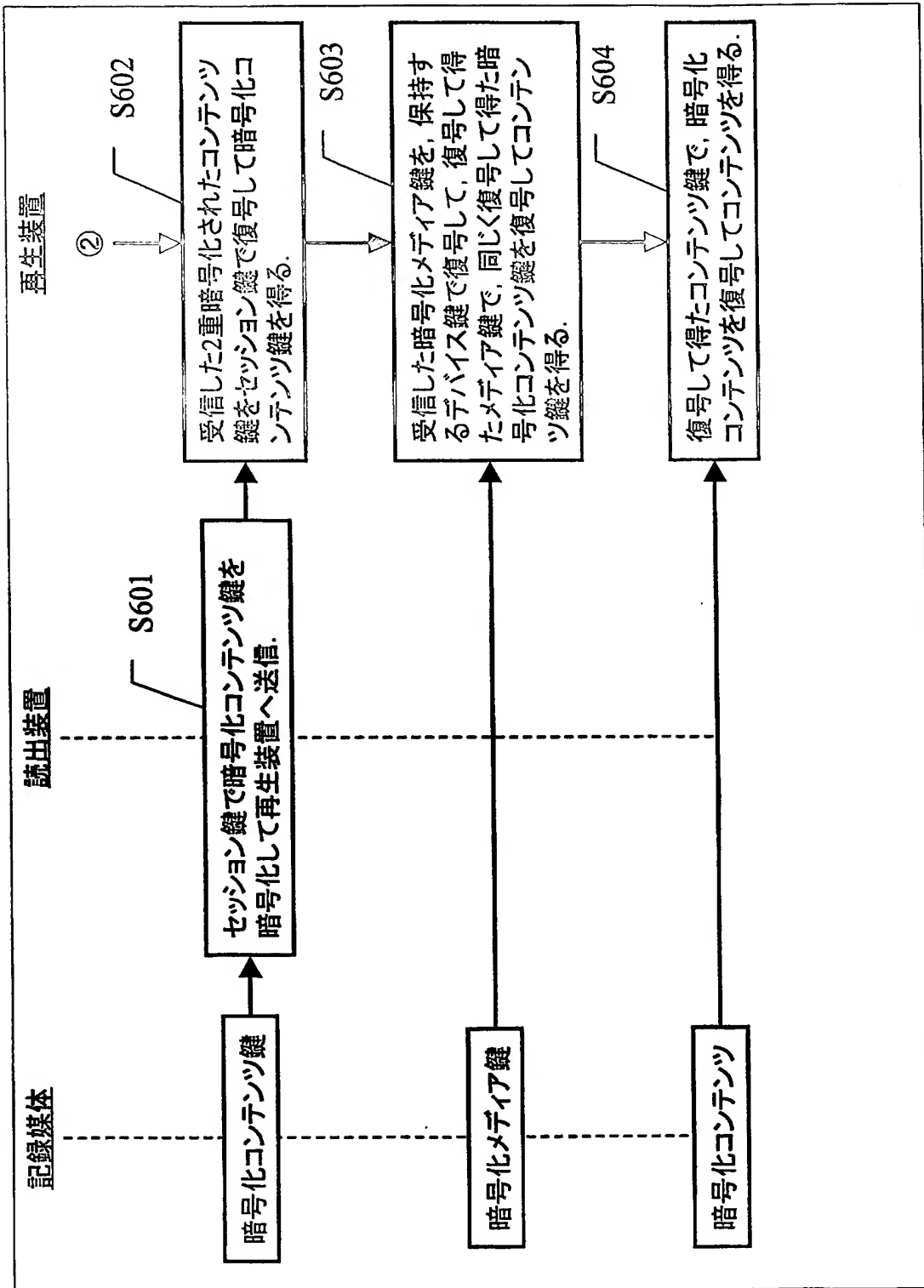
【図 4】



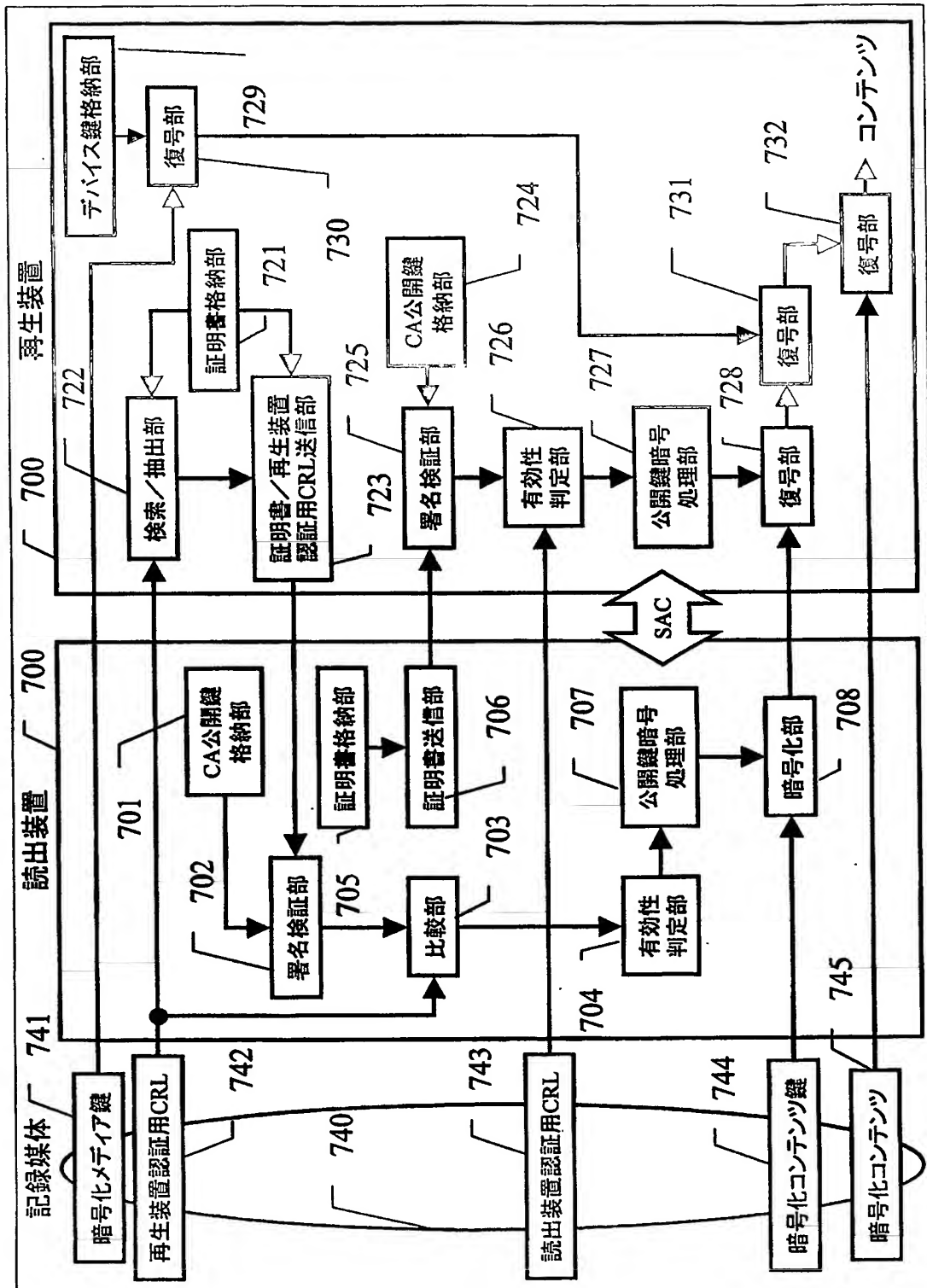
【図5】



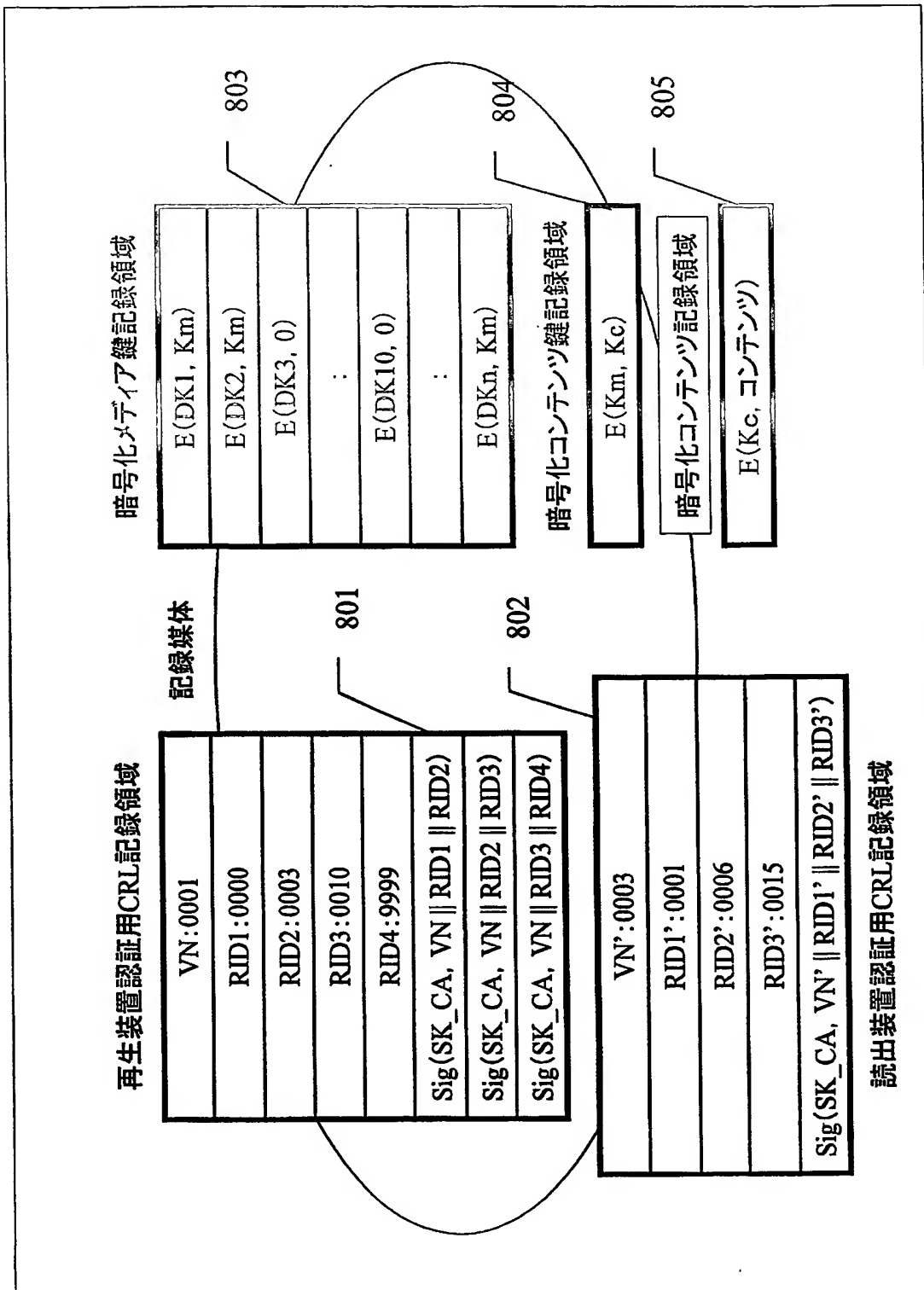
【図 6】



【図7】

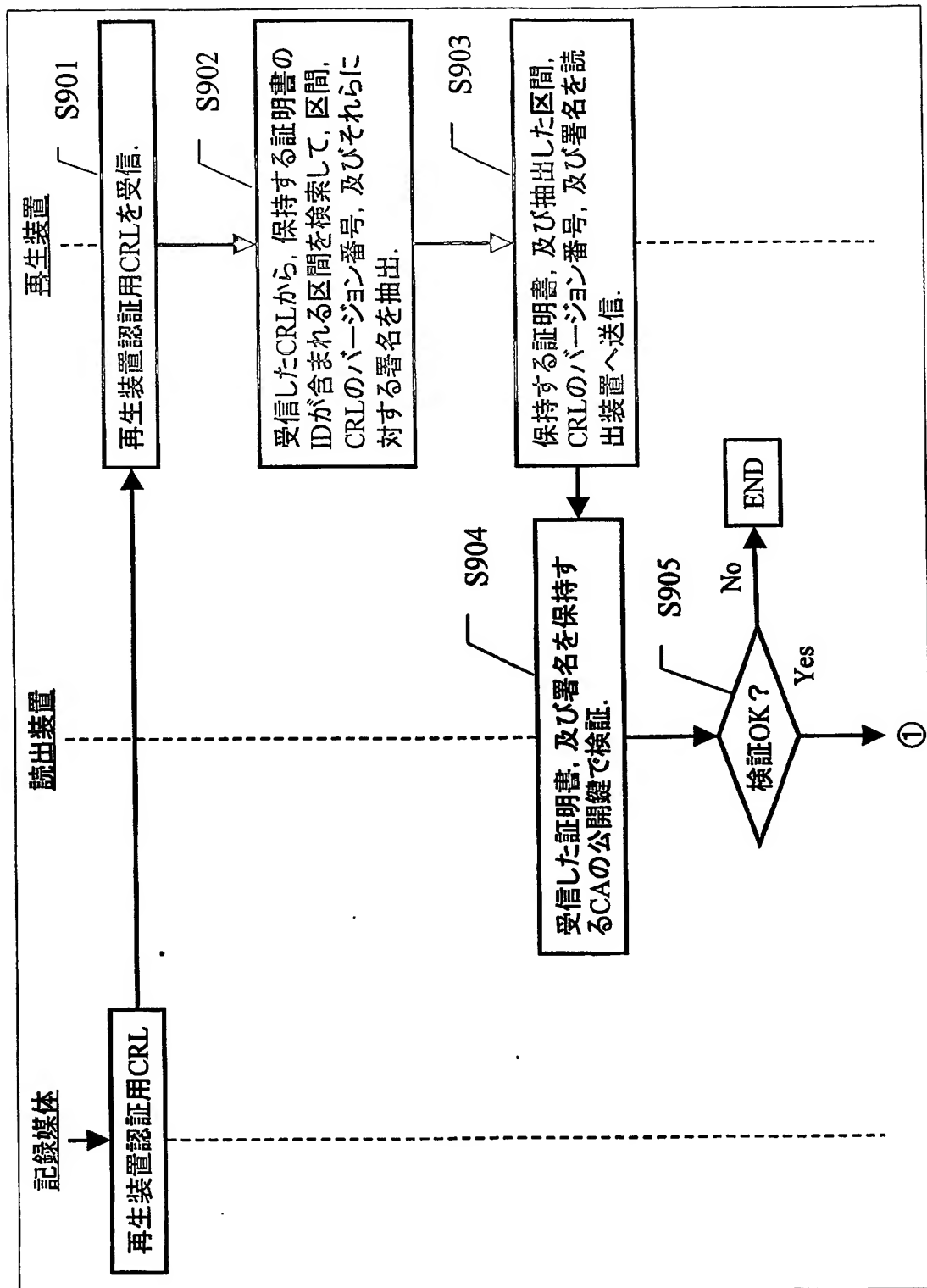


【図 8】

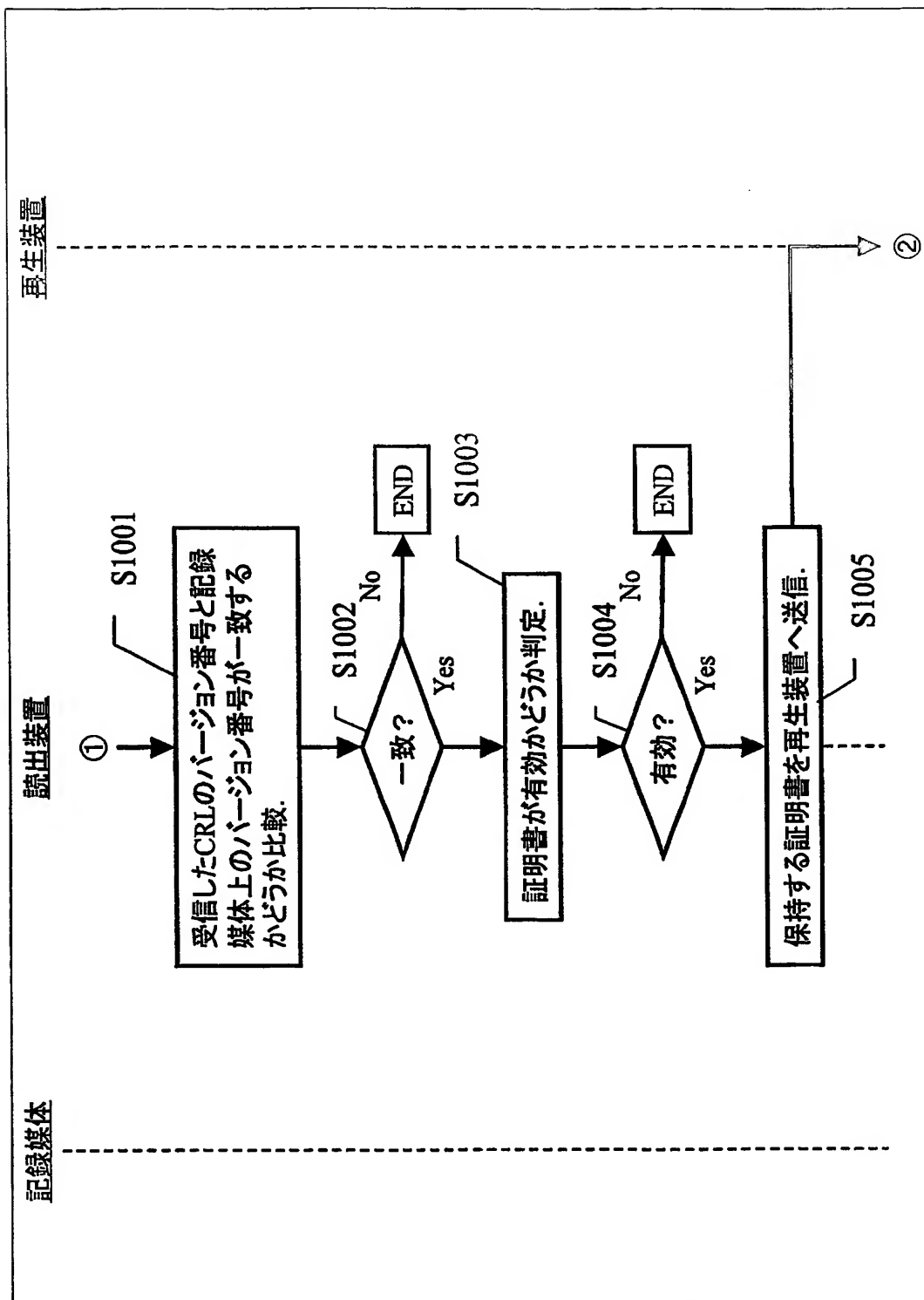




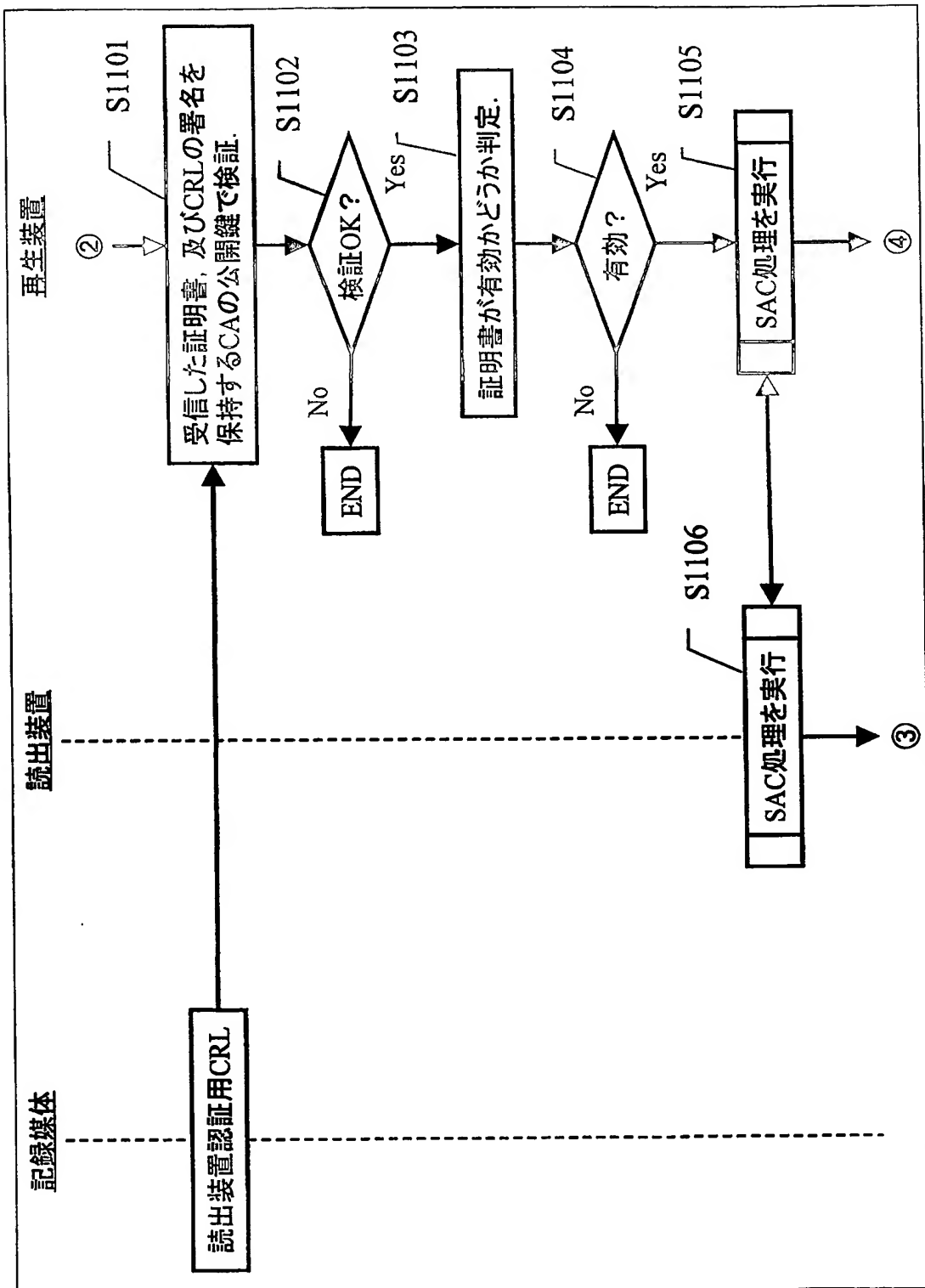
【図 9】



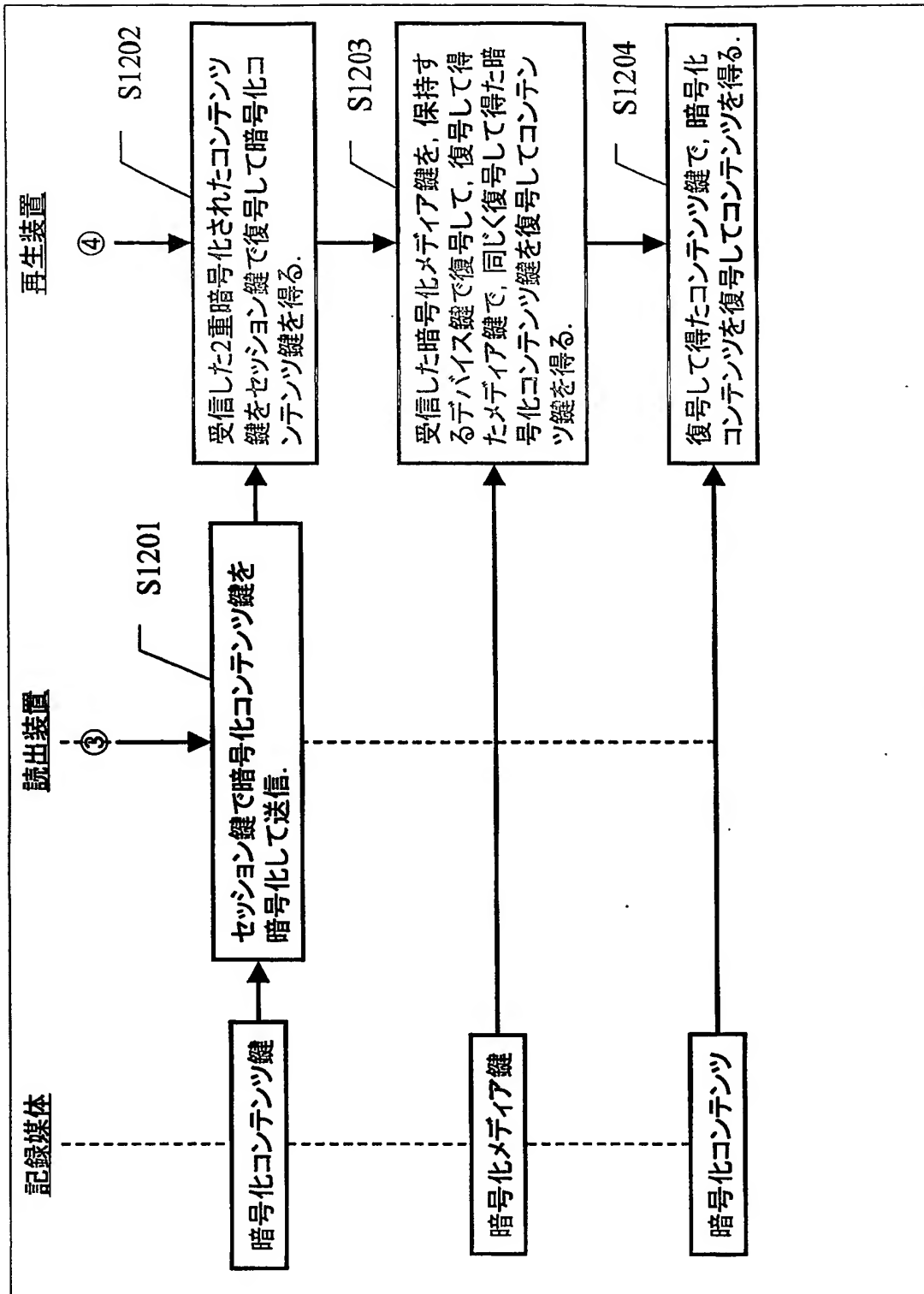
【図 10】



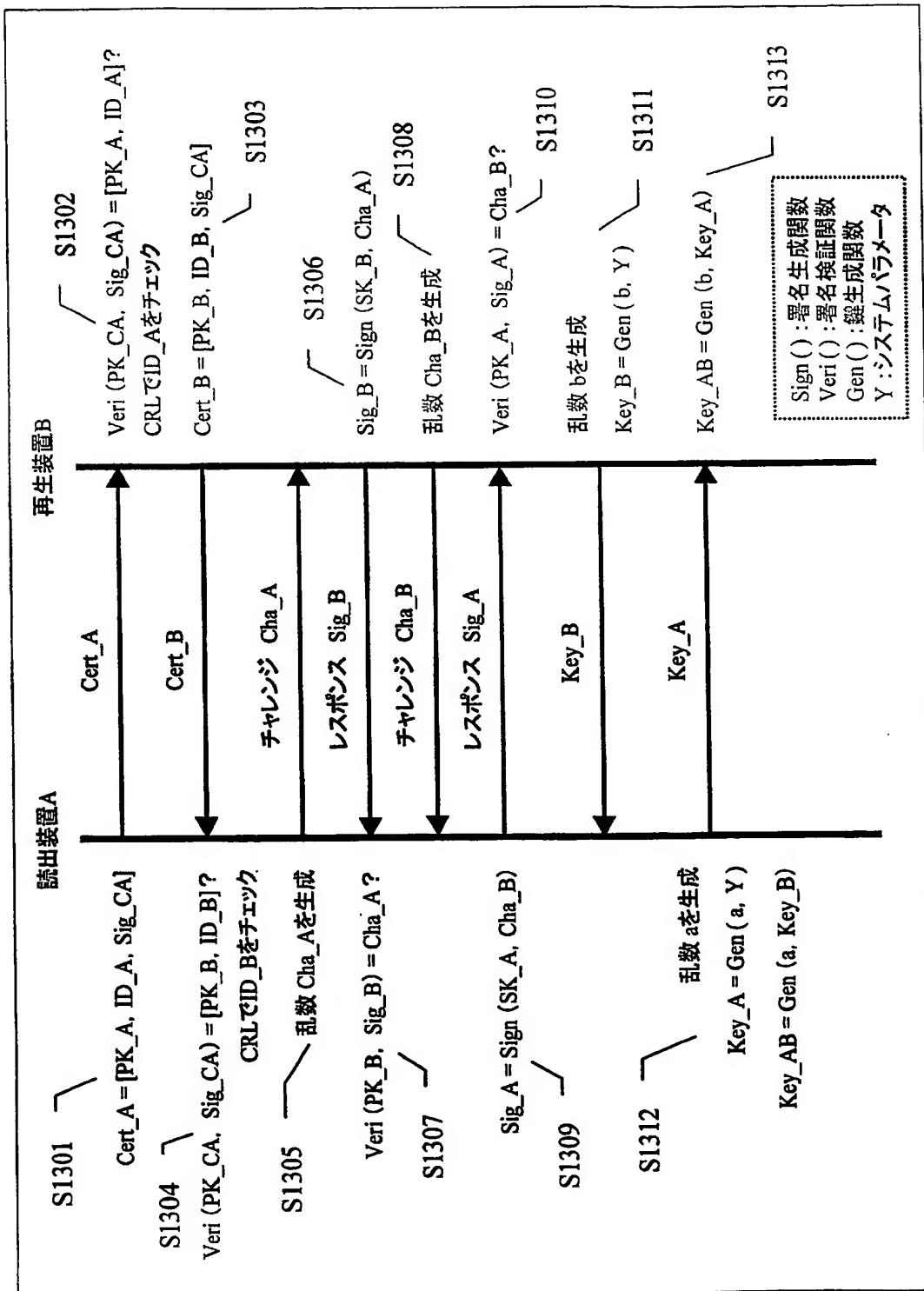
【図 11】



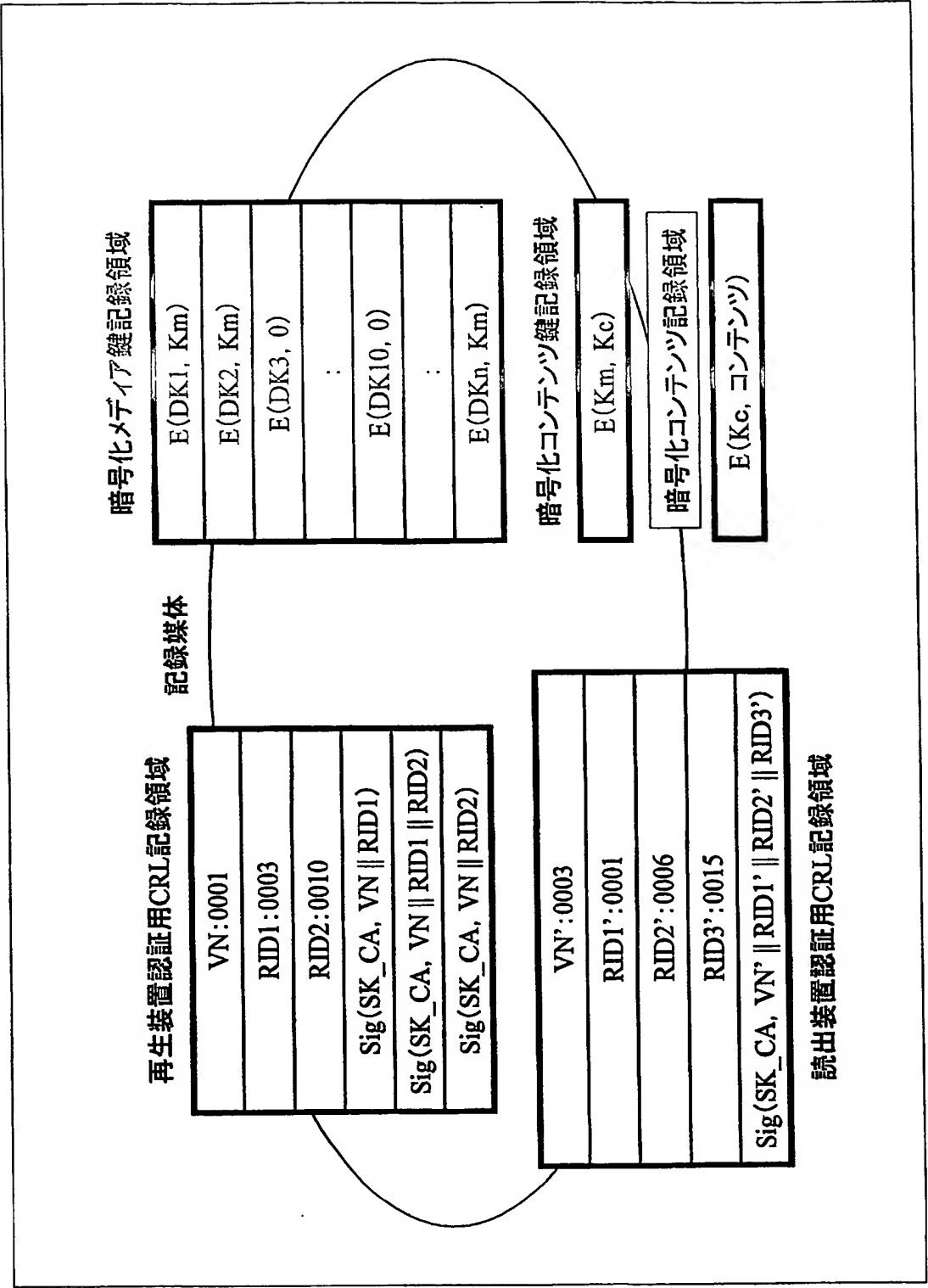
【図 12】



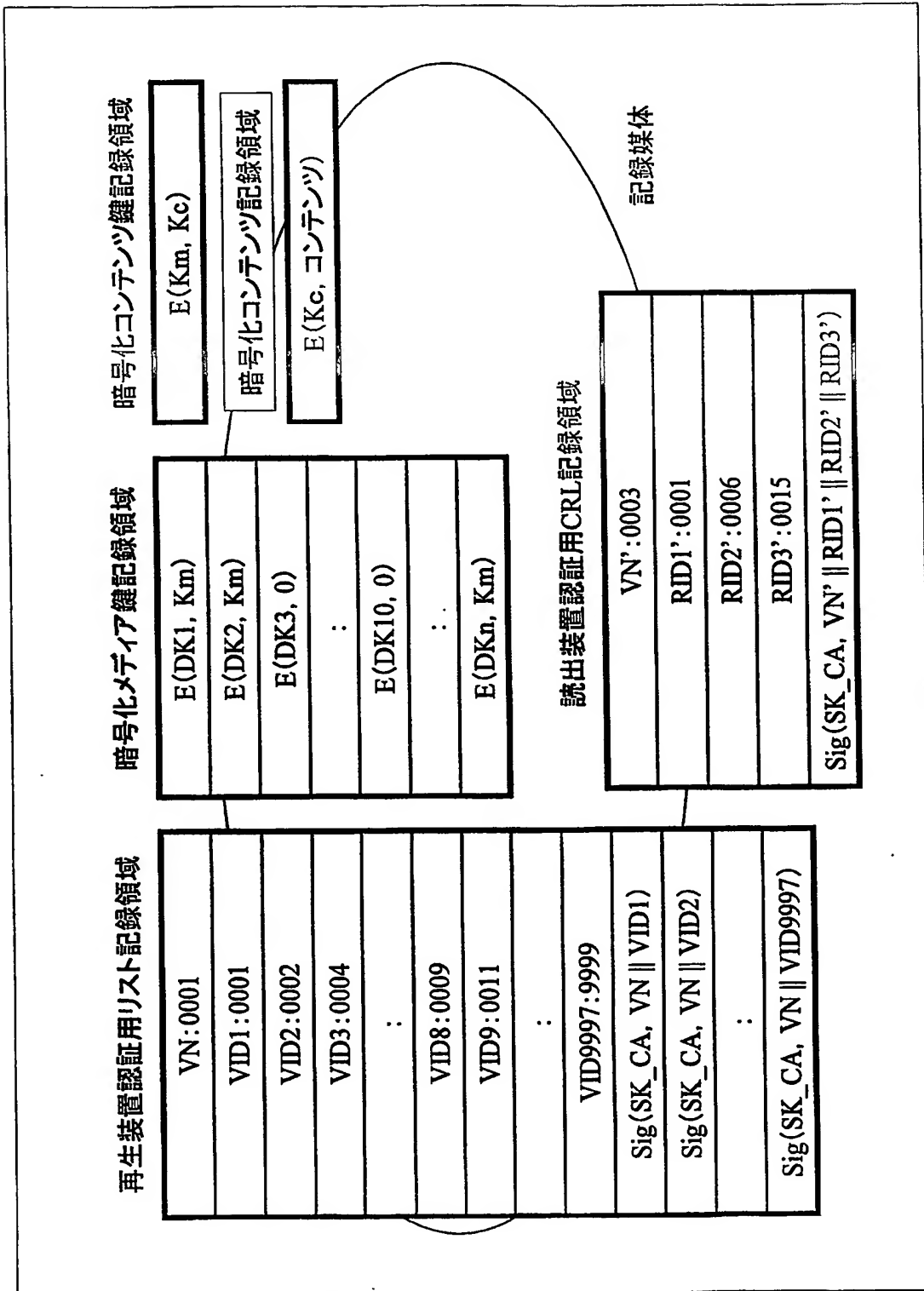
【図 13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 公開鍵暗号を利用した認証システムにおいて、C R Lのサイズが大きくなった場合であってもドライブの処理負荷を軽減する。

【解決手段】 ドライブがホストを認証する場合であっても、ホストがC R Lを検索してドライブに結果を送信し、その検索結果を受信したドライブが、検索結果の正当性を検証するのみでホストの認証を実現することにより、認証システムにおけるドライブの処理負荷を軽減する。

【選択図】 図 1



特願 2 0 0 3 - 2 7 1 9 2 9

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日 1 9 9 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 大阪府門真市大字門真 1 0 0 6 番地

氏 名 松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**